We claim:

1. A method of generating an elliptic curve, comprising:
selecting a discriminant;
determining a class polynomial; and
constructing an elliptic curve based on the selected discriminant and class polynomial.

2. The method of claim 1, further comprising storing a set of discriminants and obtaining the selected discriminant from the set of discriminants.

3. The method of claim 2, further comprising storing a set of class polynomials and obtaining the selected class polynomial from the set of class polynomials.

4. The method of claim 1, further comprising storing a set of class polynomials and obtaining the selected class polynomial from the set of class polynomials.

5. The method of claim 1, further comprising adjusting an order of the constructed elliptic curve.

6. The method of claim 5, wherein the order of the elliptic curve is adjusted by forming a twist of the elliptic curve.

7. A computer readable medium that includes computer-readable instructions for performing the method of claim 6.

8. A computer readable medium that includes computer-readable instructions for performing the method of claim 1.

9. The method of claim 1, further comprising:
selecting a prime number based on the selected discriminant; and
determining an order of the constructed elliptic curve based on the prime number.

10. A cryptographic method, comprising:
requesting construction of an elliptic curve; and
providing an elliptic curve based on a selected discriminant.

11. A computer readable medium that includes computer-readable instructions for performing the method of claim 10.

12. The method of claim 10, further comprising obtaining a class polynomial, wherein the elliptic curve is based on a root of the class polynomial.

13. A cryptographic processor, comprising an elliptic curve generator configured to provide an elliptic curve based on a discriminant.

14. The processor of claim 13, further comprising discriminant memory configured to store a set of discriminants.

15. The processor of claim 14, further comprising a polynomial memory configured to store a set of class polynomials.

16. The processor of claim 15, wherein the elliptic curve generator is configured to generate the elliptic curve based on a stored discriminant and a stored class polynomial.

17. A cryptographic system, comprising a processor situated and configured to determine a set of discriminants and an associated set of class polynomials.

18. The system of claim 17, wherein the processor is configured to determine an order of an elliptic curve based on a selected discriminant of the set of discriminants.

19. An elliptic curve generator, comprising:
an input configured to receive an instruction to produce an elliptic curve;
a processor that constructs the elliptic curve based on a selected discriminant.

20. The elliptic curve generator of claim 19, wherein the processor is configured to receive the selected discriminant from a set of discriminants.

21. The elliptic curve generator of claim 20, further comprising a twist component that produces a twist of an elliptic curve.